REMARKS

This Application has been carefully reviewed in light of the final Office Action mailed March 14, 2005. Claims 1-3, 5, 7-29, 33-46, 48, 49, 53-57, 59, 62-67, and 70-78 were pending in this patent application. The Examiner rejects Claims 1-3, 5, 7-29, 33-46, 48, 49, 53-57, 59, 62-67, and 70-78. Applicant respectfully requests reconsideration and favorable action in this case.

Interview Summary

Applicant appreciates the courtesy of a telephone interview allowed with the Examiner on June 14, 2005. During the interview, the Applicant's attorney and the Examiner discussed the patentability of the independent claims in light of the present rejection. During that interview, the Examiner expressed to the Applicant's attorney the similarities he believed to exist between the digital signature claimed in the independent claims of the present invention and the encryption technique disclosed in *Challener*. As is discussed below, Applicant has provided a declaration describing the differences between these two concepts and thus explaining why the present claims are allowable over the cited references.

The Claims As Amended Are Allowable

The Examiner rejects Claims 1, 5, 8-11, 14-16, 18-25, 26-27, 34-37, 40-46, 48, 49, 53, 56-57, 59, 62, 65, 66, 71, and 74-78 under U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,081,793 issued to Challener, et al. ("*Challener*") in view of the publication "The Caltech/MIT Voting Technology Project," hereinafter ("*VTP*").

Claim 1 of the present application, as amended, recites the following:

An advanced voting system, comprising:
an election key generator operable to generate an election key storing information related to a voter and storing a digital signature used to ensure that the election key is valid and authentic;
one or more computing devices operable to:
interface with the election key;
retrieve the digital signature from the election key to ensure that the election key is valid and authentic;
present ballot questions to the voter if an appropriate digital signature is retrieved from the election key; and
receive interactive voter selections from the voter; and

a ballot generator operable to generate tangible ballots containing the voter selections.

Claims 27, 48, and 49, as amended, recite similar, although not identical, limitations.

Neither *Challener* nor *VTP* disclose a system that includes an election key generator that is operable to store, on an election key, *a digital signature used to ensure that the election key is valid and authentic.* These references also do not disclose one or more computing devices that are operable to present ballot questions to the voter *if an appropriate digital signature is retrieved from the election key*, as recited in amended Claim 1, and similarly in amended Claims 27, 48, and 49.

In order to establish a *prima facie* case of obviousness, three criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference, or the combination of references, must teach or suggest all of the claim limitations. *See* M.P.E.P. § 2142.

Under this standard for determining obviousness, Claims 1, 27, and 48-49 are patentable over the art of record because none of the references alone or in combination disclose, teach, or suggest each and every element of the above-identified claims. In the Office Action, the Examiner asserts that *Challener* discloses the recited limitations at Column 7, line 35 through Column 8, line 10. As noted by the Examiner this passage relates to the use of encryption to send information securely. However, this is not a disclosure of the recited limitations of Claims 1, 27, 48, and 49 for at least two reasons.

First, the encryption technique described in *Challener* is *not* a digital signature. As an example only, and not by way of limitation, the present Application describes the use of digital signatures as follows:

> The election key 20 may be encoded with a digital signature 22 of a specific election judge. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of the

document. A digital signature is used to ensure that the original content of the message or document that has been sent is unchanged. Digital signature 22 may be specific to the particular precinct at which the voter is authorized to vote and may be stored in data storage location 16. Election key 20 may be a bar coded card, a magnetic stripe card, an optical disc (such as a CD-RW or CD-ROM), a magnetic disc (such as a floppy disk), or any other suitable data storage medium operable to be encoded with digital signature 22 and/or any other appropriate information allowing a voter to vote at a voting booth 24. The digital signature 22 encoded on election key 20 may be decoded by the computing device 12 on which the voter makes his voting selections to ensure that the voter does not substitute a different ballot from the one the voter is authorized to use.

(Page 8, line 27 – Page 9, line 8).

As is described in the Application, the use of a digital signature is not similar to the use of encryption in *Challener*. Applicant has provided a declaration to further explain the differences between encryption and a digital signature. Applicant directs the Examiner to that declaration for further explanation.

Second, the system disclosed in *Challener* does not use the disclosed encryption technique to store any information that is retrieved from an election key by a computing device to ensure that the election key is valid and authentic and the *Challener* system also does not present ballot questions to the voter based on whether an appropriate digital signature is retrieved from the election key.

Furthermore, although not described in the Office Action, the Examiner also asserted during the telephone interview that *VTP* also discloses the use of a digital signature on an election key at page 61, column 1, paragraph 5. However, *VTP* discloses that the completed *ballot*, not the *election key*, contains a digital signature. Therefore, it does not disclose "one or more computing devices operable to: interface with the election key; retrieve the digital signature from the election key to ensure that the election key is valid and authentic; [and] present ballot questions to the voter if an appropriate digital signature is retrieved from the election key." Since the digital signature is not added until the ballot is completed, it cannot be used to ensure that an election key is valid and authentic before presenting ballot questions to the voter.

For at least these reasons and the reasons provided in Applicant's declaration, Claims 1, 27, and 48-49, as amended, are allowable over the cited references. Therefore, Applicant respectfully requests reconsideration and allowance of Claims 1, 27, and 48-49 and all claims that depend from those claims.
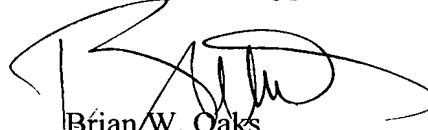
CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicant respectfully requests full allowance of all pending claims.

If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the Examiner is invited to contact Brian W. Oaks, Attorney for Applicant, at the Examiner's convenience at (214) 953-6986.

Enclosed are checks in the amount of $395.00 for filing the Request for Continued Examination, and $510.00 for a three-month extension of time. The Commissioner is hereby authorized to charge any fee and credit any overpayment to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Brian W. Oaks
Reg. No. 44,981

Date: September 13, 2005

Correspondence Address:

Customer Number: 05073

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Sanford J. Morganstein

Serial No.:   10/001,511

Filing Date: October 31, 2001

Examiner: Daniel A. Hess

Group Art Unit: 2876

Title: Advanced Voting System and Method

Commissioner of Patents

P.O. Box 1450

Alexandria, VA 22313-1450

DECLARATION OF SANFORD J. MORGANSTEIN UNDER 37 C.F.R. §1.132

I, Sanford J. Morganstein, declare as follows:

1.   I am over the age of 21 years, of sound mind, and competent in all respects to make this declaration.

2.   I have been informed of the examiner's comments with respect to the Challener reference and its purported disclosure of a digital signature as recited in the claims of the above-referenced application. Specifically, I understand that the examiner is equating the public key/private key encryption process described at Column 3, line 29 through Column 4, line 15 of the Challener reference with the claimed digital signature. As described below, I believe equating the use of Public key/Private key encryption with the use of a digital signature is incorrect.

3. In general, encryption is used to prevent reading a secret document by an unauthorized person. On the other hand, signing (including digital signing) is used to assure authenticity of the creator of the document. These distinctions have their counterparts in everyday activities. Consider for example a bank check. When a check is set in the mail, it is placed in a sealed envelope so that an unauthorized person cannot read its contents. Quite a different function is performed by the check maker's signature. The signature identifies the maker and has nothing to do with obscuring the contents of the check.

4. These points are mode clear in the glossary in to the book, "the Code Book" by Simon Singh, Ph. D.; published by Anchor Books, 1999 (excerpts attached as Appendix A). Dr. Singh defines "Cryptology" as "the science of **secret** writing in all it forms, covering both cryptography and cryptanalysis" (emphasis added).[1] Dr. Singh defines "Digital Signature" as "a method for proving the **authorship** of an electronic document" (emphasis added). He goes on to state that a digital signature often "is generated by the author encrypting the document with his or her private key." Thus, encryption (concealing a message) and digital signing (proving authenticity) may use similar tools based on the science of cryptography for very different purposes.

5. Public and private keys are modern tools used for the functions of concealment and authenticity verification. But, encryption and digital signing can be performed without Public/Private key technology. The following is an example of encryption that does not use public/private key technology. Consider the following simple message to be sent to an ally when it is important that an unauthorized person not understand the message:

ATTACK FROM EAST AT DAWN

Before sending the message, the author changes each letter in the message shown in the top line of the table, below, with the letter shown in the second row.

---

[1] Dr. Singh defines "Cryptanalysis" as "the science of deducing the plaintext from a ciphertext, without knowledge of the key."

```
A B C D  E  F G H I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
B C D E  F  G H I J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z  A
```

Using this simple encryption method in which each letter is replaced by a different letter of the alphabet (a simple substitution cipher), the message becomes:

BUUBDL GSPN FBTU BU EBXO

Unless the recipient of the message knew that each letter of the original message was substituted according to the table shown above, it would be extremely difficult for the recipient to understand the message. If all members of an allied group used the same key, all members of that allied group could encrypt a message the same way without authenticating the identity of the sender. All members of the allied group could decipher a message encrypted with the key known to them.

6. The following is an example of creating a digital signature without public/private key technology. Consider the following example in which it is not important to conceal the contents of the message but it is important to identify the creator of the message:

MEET ME AT NOON

The creator of the message can design a key assigning a value to each letter of the alphabet as follows (the example is a particularly poor encoding since it is easy to guess, but any number of different encodings, or keys, could be used):

```
A B C D  E  F G H I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
1 2 3  4   5  6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The message creator could then add a number to the end of the message which is the sum of the key values. With M=13, E= 5, etc., the values of each of the letters of the message is (ignoring spaces):

    ME E T   ME A T N O O N
    13 5 5 20 13 5 1 20 14 15 15 14

Calculating the sum of all the substituted values results in 140. The number (140 in this case) serves as a kind of digital signature (sometimes also called a "hash"). Without obscuring the contents of the message, the message sender could send the following:

    MEET ME AT NOON 140

If the recipient of the message knew the substitution values used by the sender, he could calculate the same sum, 140, and in matching the 140 sent *with* the message (the digital signature) to the calculated value (140) the recipient could have a reasonable assurance that the message had been sent by the ally. Note that this method also assures that the message has not been tampered with. If the message had been tampered with, the malicious person who tampered with the message would have to know the key, i.e. the substitution values, to come up with a number at the end, or digital signature, that the key and calculation produces.
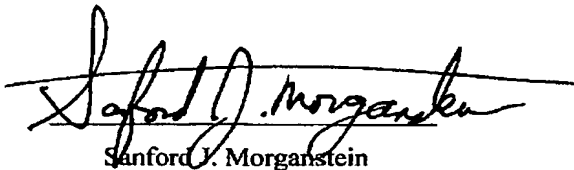
7.   Note that both the first example (used to obscure the contents of a message) and the second example (used to authenticate the contents and the sender) use a substitution key to perform widely different functions. This difference in function differentiates the present invention (used for authentication) from Challener (used for privacy). Public/Private key technology could be used to encrypt a message and to create a digital signature. But, regardless of the technologies used, the functions are different. Public/Private key technology solves a problem tangential to the authenticity issue solved by the present invention. Public/Private key technology solves the problem of providing a method for the message author to send private messages without worrying about how to send a secret decryption key to the recipient. In

Public/Private key technology, two keys are involved, a Public Key (which anyone can know) and a Private Key, known only to one of the communicants.

8.   Although both encryption and digital signing can be performed using Public/Private key technology, the use of Public/Private key technology does not imply that both encryption and digital signing are being performed.   In fact, the Challener reference only describes that Public/Private key technology is used to provide encryption (see Column 3, line 66 through Column 4, line 5 – "one or more cryptographic operations are utilized to encrypt data flows"). It does not describe using Public/Private key technology to create a digital signature (or using any other technique to create a digital signature).

9.   I hereby declare that all statements made herein are of my own knowledge, are true, and that all statements made on information and belief are believed to be true; and further, that the statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this affidavit is directed.

Dated this 10th day of September 2005.

Sanford J. Morganstein

APPENDIX A

THE CODE BOOK

THE SCIENCE OF SECRECY
FROM ANCIENT EGYPT TO
QUANTUM CRYPTOGRAPHY

NATIONAL BESTSELLER

"It would be hard to imagine a clearer or more fascinating presentation.... Mr. Singh gives cryptography not only its historical dimension but its human one."
—*THE NEW YORK TIMES*

SIMON SINGH

Bestselling Author of FERMAT'S ENIGMA

For my mother and father,

Sawaran Kaur and Mehnga Singh

Glossary

ASCII American Standard Code for Information Interchange; a standard for turning alphabetic and other characters into numbers.

asymmetric key cryptography A form of cryptography in which the key required for encrypting is not the same as the key required for decrypting.

Describes public key cryptography systems, such as RSA.

Caesar-shift substitution cipher Originally a cipher in which each letter in the message is replaced with the letter three places further on in the alphabet. More generally, it is a cipher in which each letter in the message is replaced with the letter *x* places further on in the alphabet, where *x* is a number between 1 and 25.

cipher Any general system for hiding the meaning of a message by replacing each letter in the original message with another letter. The system should have some built-in flexibility, known as the key.

cipher alphabet The rearrangement of the ordinary (or plain) alphabet, which then determines how each letter in the original message is enciphered. The cipher alphabet can also consist of numbers or any other characters, but in all cases it dictates the replacements for letters in the original message.

ciphertext The message (or plaintext) after encipherment.

code A system for hiding the meaning of a message by replacing each word or phrase in the original message with another character or set of characters. The list of replacements is contained in a codebook. (An alternative definition of code is any form of encryption which has no built-in flexibility, i.e., there is only one key, namely the codebook.)

codebook A list of replacements for words or phrases in the original message.

cryptanalysis The science of deducing the meaning of a ciphertext, without knowledge of the key.

cryptography The science of encrypting a message, or the science of concealing the meaning of a message. Sometimes the term is used more generally to mean the science of anything connected with ciphers, and is an alternative to the term cryptology.

391

cryptology The science of secret writing in all its forms, covering both cryptography and cryptanalysis.

decipher To turn an enciphered message back into the original message.

decode To turn an encoded message back into the original message.

DES Data Encryption Standard, developed by IBM and adopted in 1976.

Diffie-Hellman-Merkle key exchange A process by which a sender and receiver can establish a secret key via a public discussion. Once the key has been agreed, the sender can use a cipher such as DES to encrypt a message.

digital signature A method for proving the authorship of an electronic document. (Often this is generated by the author encrypting the document with his or her private key.)

encipher To turn the original message into the enciphered message by scrambling its contents.

encode To turn the original message into the encoded message.

encrypt To encipher or encode.

encryption Any general encryption process which can be specified exactly by choosing a key.

homophonic substitution cipher A cipher in which there are several potential substitutions for each plaintext letter. Crucially, if there are, say, six potential substitutions for the plaintext letter a, then these six characters can only represent the letter a.

Key The element that turns the general encryption algorithm into a specific method for encryption. In general, the enemy may be aware of the encryption algorithm being used by the sender and receiver, but the enemy must not be allowed to know the key.

Key distribution The process of ensuring that both sender and receiver have access to the key required to encrypt and decrypt a message, while making sure that the key does not fall into enemy hands. Key distribution was a major problem in terms of logistics and security before the invention of public key cryptography.

key escrow A scheme in which users lodge copies of their secret keys with a trusted third party, the escrow agent, who will pass on keys to law enforcers only under certain circumstances, for example if a court order is issued.

key length Computer encryption involves keys which are numbers. The length refers to the number of digits or bits in the key, and thus indicates the biggest number that can be used as a key, thereby defining the number of possible keys. The longer the key length (or the greater the number of possible keys), the longer it will take a cryptanalyst to search all the keys.

monoalphabetic substitution cipher A substitution cipher in which the cipher alphabet is fixed throughout encryption.

National Security Agency (NSA) A branch of the U.S. Department of Defense, responsible for ensuring the security of America's communications and for breaking into the communications of other countries.

one-time pad cipher The only known form of encryption that is unbreakable. It relies on a random key that is the same length as the message. Each key can be used once and only once.

plaintext The original message before encryption.

polyalphabetic substitution cipher A substitution cipher in which the cipher alphabet changes during the encryption, for example the Vigenère cipher. The change is defined by a key.

Pretty Good Privacy (PGP) A computer encryption algorithm developed by Phil Zimmermann, based on RSA.

private key The key used by the receiver to decrypt messages in a system of public key cryptography. The private key must be kept secret.

public key The key used by the sender to encrypt a message in a system of public key cryptography. The public key is available to the public.

public key cryptography A system of cryptography which overcomes the problems of key distribution. Public key cryptography requires an asymmetric cipher, so that each user can create a public encryption key and a private decryption key.

quantum computer An immensely powerful computer that exploits quantum theory, in particular the theory that an object can be in many states at once (superposition), or the theory that an object can be in many universes at once. If scientists could build a quantum computer, it would jeopardize the security of all current ciphers, except the one-time pad cipher.

quantum cryptography An unbreakable form of cryptography that exploits quantum theory, in particular the uncertainty principle, which states that it is impossible to measure all aspects of an object with absolute certainty. Quantum cryptography guarantees the secure exchange of a random series of bits, which in turn can be used as the basis for a one-time pad cipher.

RSA The first system that fitted the requirements of public key cryptography, invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1977.

steganography The science of hiding the existence of a message, as opposed to cryptography, which is the science of hiding the meaning of a message.

substitution cipher A system of encryption in which each letter of a message is replaced with another character, but retains its position within the message.

symmetric key cryptography A form of cryptography in which the key required for encrypting is the same as the key required for decrypting. The term describes all traditional forms of encryption, i.e. those in use before the 1970s.

transposition cipher A system of encryption in which each letter of a message changes its position within the message, but retains its identity.

Vigenère cipher A polyalphabetic cipher which was developed around 1500. The Vigenère square contains 26 separate cipher alphabets, each one a Caesar-shifted alphabet, and a keyword defines which cipher alphabet should be used to encrypt each letter of a message.

Acknowledgments